IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

AF
TC

Applicant: A. Kent Sievers et al.

Title: METHODS, DATA STRUCTURES AND SYSTEMS TO REMOTELY VALIDATE A MESSAGE

Docket No.: 1565.006US1
Filed: March 6, 2002
Examiner: David G. Cervetti

Serial No.: 10/092,822
Due Date: March 5, 2007
Group Art Unit: 2136

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

X Appeal Brief Under 37 CFR 41.37 (22 pgs.) including authorization to charge Deposit Account 19-0743 in the amount of $500.00 to cover the Appeal Fee.
X Return postcard.

If not provided for in a separate paper filed herewith, Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: /Joseph P. Mehrle/
Atty: Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 5 day of March, 2007.

Peter Rebuffoni
Name

Signature

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants: A. K. Sievers et al. Examiner: David G. Cervetti

Serial No.: 10/092,822 Group Art Unit: 2136

Filed: March 06, 2002 Docket: 1565.006US1

Title: METHODS, DATA STRUCTURES AND SYSTEMS TO REMOTELY VALIDATE A MESSAGE

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

The Appeal Brief is presented in response to the Notice of Panel Decision from Pre-Appeal Brief Review mailed on February 5, 2007 and further in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on December 28, 2006, from the Final Rejection of claims 1-20 of the above-identified application, as set forth in the Final Office Action mailed on October 24, 2006.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of $500.00 which represents the requisite fee set forth in 37 C.F.R. § 41.20(b)(2). The Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims.

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, NOVELL, INC. as evidenced by the assignment from the inventors recorded March 6, 2002 at Reel 012682, Frame 0154.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants that will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

The present application was filed on March 6, 2002 with claims 1-26. In response to a non-final Office Action mailed May 10, 2006, Appellants canceled claims 21-26. A Final Office Action (hereinafter "the Final Office Action") was mailed October 24, 2006. Claims 1-20 stand twice rejected, remain pending, and are the subject of the present Appeal.

4. STATUS OF AMENDMENTS

No amendments have been made subsequent to the Final Office Action mailed October 24, 2006.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Some aspects of the present inventive subject matter include, but are not limited to, methods, data structures, and systems to remotely validate a message.

INDEPENDENT CLAIM 1

1. A method to remotely validate an email message, comprising: *[FIG. 1; specification pages 7-9 first full paragraph]*

receiving, at a recipient, the email message in a first encrypted format from a sender of the email message, wherein the recipient is whom the email message is directed to for consumption; *[FIG. 1 reference numeral 110 and specification page 7 second full paragraph]*

decrypting, at the recipient, contents of the email message from the first encrypted format; *[FIG. 1 reference numeral 120 and specification page 7 penultimate paragraph]*

transferring, from the recipient, the decrypted email message contents to a remote server; and *[FIG. 1 reference numeral 130 and specification page 7 penultimate paragraph and continuing through page 8 through first cull and complete paragraph]*

receiving, at the recipient, from the remote server a status flag, wherein a value associated with the status flag indicates whether the contents are free from a virus or are free from objectionable material as validated by the remote server. *[FIG. 1 reference numeral and specification page 8 penultimate paragraph and continuing through first full paragraph page 9]*

INDEPENDENT CLAIM 7

7. A method to validate a data message, comprising: [FIG. 3 and specification pages 10 and 11 through second full paragraph]

receiving the data message from a client, wherein the data message was previously received at the client and sent from a sender of the data message to the client, wherein the client decrypts the data message before the data message is processed by the client, and wherein the client is external and remote to the method and communicates with the method over a network by sending the data message for scanning, and wherein the client is who the data message is directed to for consumption; *[FIG. 3 references numerals 310, 320, 330, 340, 350, and 355 and specification page 10 penultimate paragraph and continuing through first paragraph page 11]*

scanning the data message for viruses; and *[FIG. 3 reference numeral 360 and specification page 11 first full paragraph]*

sending a validation flag to the client, wherein the validation flag includes a value indicating whether the data message includes zero or more of the viruses. *[FIG. 3 reference numerals 370 and 380 and specification page 11 second full paragraph]*

INDEPENDENT CLAIM 14

14. An email system to validate an email message, comprising: *[FIGS. 4 and 5 and specification page 11 penultimate paragraph and continuing to page 14 first full paragraph]*

a local email set of executable instructions residing on a client; *[FIG. 4 reference numeral 412 and specification page 11 penultimate paragraph; FIG. 5 reference numeral 530 and specification page 13 first two and complete paragraphs]*

a remote validation set of executable instructions residing on a server; and *[FIG. 4 reference numeral 422 and specification page 11 penultimate paragraph and continuing through page 12; FIG. 5 reference numeral 550 and specification page 13]*

wherein the email message is received by the local email set of executable instructions from a sender, who intends the email message for the client and the client is who the email message is directed to for consumption, and local email set of executable instructions decrypts the email message and then streams the email message to the remote validation set of executable instructions located on the server in an unencrypted format or in a different encrypted format from what was received on the client from the sender and wherein the email message is scanned and a validation flag associated with a result of the scan is sent to the local email set of

executable instructions back on the client. *[FIGS. 4 and 5 and specification page 11 penultimate paragraph and continuing to page 14 first full paragraph]*

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and its legal equivalents for a complete statement of the invention.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

§103 Rejection of the Claims

Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hruska et al. (U.S. 6,195,587 –herein after Hruska) in view of Ranger et al. (U.S. 6,393,568 – herein after Ranger).

7. ARGUMENT

A) The Applicable Law under 35 U.S.C. §103(a).

To sustain a rejection under 35 U.S.C. 103, references must be cited that teach or suggest all the claim elements. M.P.E.P. § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983); *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985); MPEP § 2141.02.

Further, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143. The Examiner must avoid hindsight. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). The Office Action must further provide specific, objective evidence of record for a finding of a suggestion or motivation to combine reference teachings and must explain the reasoning by which the evidence is deemed to support such a finding. *In re Sang Su Lee*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002).

Appellants would further like to point out that the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art recited also suggests in some manner the desirability of the proposed combination. *In re Mills*, 916 F.2d 680, 16 USPQ 2d 1430 (Fed. Cir. 1990). Appellants would also like to note that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *See Lee*, 277 F.3d 1338, 1343-46 (Fed. Cir. 2002); *Rouffet*, 149 F.3d 1350, 1355-59 (Fed. Cir. 1998). This requirement is rooted in the Administrative Procedure Act, which ensures due process and non-arbitrary decision making, as it is in 35 U.S.C. § 103. See id, at 1344-45." *In re Kahn*, No. 04-1616 (Fed. Cir. March 22, 2006).

It has also been held that when the primary teachings of one reference is negated or taught against or taught away from another reference in the proposed combination, then it is common sense that one of ordinary skill in the art would not have been motivated to combine the references in the manner being proposed, because in so doing the very teachings that are asserted to be complimentary are by definition not complimentary to one another. Thus, there is no motivation by one of ordinary skill in the art to combine the references. It is also the case that the intended functions of the references being combined cannot be destroyed when combined. *See In re Grasselli*, 713 F.2d 731, 743; 218 USPQ 769, 779 (Fed. Cir. 1983).

B) Discussion of the rejection of claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hruska in view of Ranger.

Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hruska in view of Ranger. This rejection is respectfully traversed, Appellant respectfully submits that the Final Office Action has made an improper prima facie showing of obviousness at least because the references standing alone or in combination fail to teach receiving an email message in a first encrypted format and transferring, for a recipient, a decrypted email; and because the proposed combination lacks motivation to be combined by one of ordinary skill in the art.

Consequently, Appellant respectfully requests reversal of the § 103(a) rejections.

Specifically, a recipient (or client) of the email receives an encrypted email in a first format from a sender. This particular limitation exists in one form or another in each of the independent claims. The Examiner has relied on Hruska for the this teaching. However, the entire teaching of Hruska lacks any discussion of encrypted email messages entirely except for column 5 lines 41-59. Here, a workstation or recipient copies a file in an encrypted format to a server that then decrypts it. The recipient of the file or the intended target or consumer of the file is the workstation and not the server, which is providing a service to the workstation. This reference entirely lacks any suggestion that the workstation receives the file from a sender in an encrypted format; it only suggests that a consumer of a file sends a file in an encrypted format.

Column 5 lines 41-43 of Hruska indicates that there are two methods by which a "file is transferred to the file server and a report message returned to the workstation. Lines 43-59

describe the scenario discussed above where an "encrypted" file is copied to the file server and the file server then periodically scans for new files in certain directories, with certain names, *etc.* The second approach is discussed at column 5 lines 60-67 and this one begins with the acknowledgment that the file is copied from the workstation to the file server in the same exact manner as the first technique (encrypted from workstation to file server). The difference with the second approach is only in how the file server becomes aware of the file to produce a checksum for; specifically, in the second approach the file server receives a packet message from the workstation to perform the checksum service. In both approaches, the file is copied in an encrypted format from the workstation to the file server. Thus, Hruska lacks any teaching or suggestion of a teaching that the file server receives the file in a decrypted format or that the workstation receives the file in an encrypted format. Consequently, the cited teaching provided by the Examiner is deficient and fails to provide a valid prima facie bases for obviousness.

Secondly, and in some ways related to the first point, the references fail to send a decrypted email or message to a service for processing. Specifically, Hruska calls for "copying" a file in an "encrypted format" to a file server. This is exactly the opposite of sending a message in a decrypted format. In fact, the Examiner appears to have acknowledged that Hruska does not teach decryption and wants to rely on Ranger for this. However, decryption cannot be taking out of context it is associated with decrypting at a recipient of an email or message that particular email or message which is then sent in a decrypted format to a service for virus scanning.

Ranger is directed to techniques for virus scanning that is performed at a firewall node prior to delivery of data to the intended recipients within a network. The data is encrypted and has to be decrypted before it can be properly scanned for viruses. As a result, Ranger discusses elaborate key exchange mechanisms, such that the file server located at the firewall can properly decrypt and in some cases re-encrypt the data being received from recipients. The techniques in Ranger require that the file server that processes or utilizes the virus scan have the knowledge to decrypt recipient specific messages. *E.g.*, col. 2 lines 51-56; col. 3 lines 15-29; col. 4 lines 1-5, and lines 53-64; col. 6 lines 7-9, 34-40, and 59-65; and col. 7 lines 20-26.

The problem with this approach is that it relies too heavily on a single application or service to decrypt all messages. This requires extensive key communication and in fact could introduce even more security risks since keys of recipients are being communicated over the

network or acquired over the network for purposes of the service being able to decrypt the messages. Appellant's approach is more portable and a less coupled technique, where the recipients use their own keys and manage their own keys securely and independent of the virus scanning process. Recipients do no view the decrypted messages; rather they forward them for virus scanning prior to inspection. In this approach, the recipient has the decrypted message and all it needs from the scanning process is a flag or indication that it can properly view the already decrypted message. In Ranger, the message is never in the possession of the intended recipient until the perimeter computer has determined it is safe for viewing at which point the message is finally delivered to the intended recipient.

So Ranger cannot teach a recipient receiving a message in encrypted format and then decrypting it for the perimeter or firewall computer.

Consequently, both Hruska and Ranger lack any teaching where a recipient or consumer of an email receives that email in encrypted format and then decrypts it and sends it to a server or service for virus scanning. Thus, the obviousness rejections should be withdrawn and the claims allowed.

Additionally, Appellants assert that the Hruska and Ranger references are not compatible with one another and as such would not have been combined by one of ordinary skill in the art because there would have been no motivation to do so because of the incompatibility. More specifically, Ranger relies and teaches a message passing technique to communicate to clients that a file is okay to read or process; whereas the Hruska reference relies on a signature or checksum value assigned to a file to communicate that the file is good to read or process. These are in fact different approaches one message passing and one signature generating. Hruska modifies the files with a signature and checksum and Ranger does not modify the files at all; rather messages are passed having key exchange information that is vital to processing the proper encryption and decryption techniques. The message passing cannot be removed from Ranger and the signature or checksum cannot be removed from Hruska. Accordingly, the proposed combination cannot be made as the two approaches are different and non complimentary and as such one of ordinary skill in the art would not have been motivated to make the combination in the first instance.

Thus, for yet another reason the rejections should be withdrawn because the proposed combination was improper. Appellant respectfully requests that the rejections be withdrawn and the claims of record be allowed to issue.

8. SUMMARY

For the reasons argued above, the claims were not properly rejected under § 103(a).

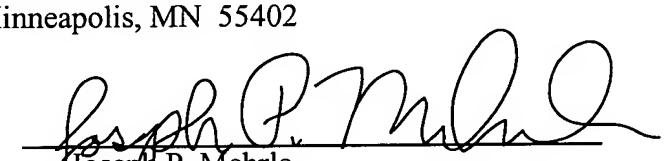
It is respectfully submitted that the art cited does not render the claims obvious and that the claims are patentable over the cited art. Reversal of the rejections and allowance of the pending claims are respectfully requested.

Respectfully submitted,

A. K. SIEVERS et al.

By their Representatives,

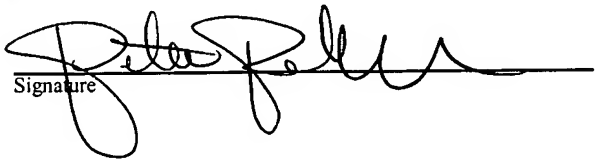
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date 03/05/07 By 

Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 5 day of March 2007.

Name Peter Rebuffoni

Signature 

CLAIMS APPENDIX

1. A method to remotely validate an email message, comprising:

receiving, at a recipient, the email message in a first encrypted format from a sender of the email message, wherein the recipient is whom the email message is directed to for consumption;

decrypting, at the recipient, contents of the email message from the first encrypted format;

transferring, from the recipient, the decrypted email message contents to a remote server; and

receiving, at the recipient, from the remote server a status flag, wherein a value associated with the status flag indicates whether the contents are free from a virus or are free from objectionable material as validated by the remote server.

2. The method of claim 1, further comprising encrypting the email message in a second encrypted format before transferring the email message to the remote server.

3. The method of claim 1, further comprising accessing the email message for use, if the value of the status flag indicates the remote server validated the email message.

4. The method of claim 1, wherein in transferring the email message, the first encrypted format is a Secure Multi-Purpose Internet Mail Extension (S/MIME) format.

5. The method of claim 1, wherein in receiving the status flag, if the value of the status flag indicates the remote server validated the email message, then subsequent accesses made to the email message do not result in the email message being transferred to the remote server for validation.

6. The method of claim 1, wherein in transferring the email message, the email message is streamed to the remote server.

7. A method to validate a data message, comprising:

receiving the data message from a client, wherein the data message was previously received at the client and sent from a sender of the data message to the client, wherein the client decrypts the data message before the data message is processed by the client, and wherein the client is external and remote to the method and communicates with the method over a network by sending the data message for scanning, and wherein the client is who the data message is directed to for consumption;

scanning the data message for viruses; and

sending a validation flag to the client, wherein the validation flag includes a value indicating whether the data message includes zero or more of the viruses.

8. The method of claim 7, further comprising decrypting the data message before scanning the data message.

9. The method of claim 8, wherein in decrypting the data message, the data message is decrypted using a public key of the client.

10. The method of claim 7, wherein in receiving the data message, the data message is an email message and the client is an email client.

11. The method of claim 7, wherein in receiving the data message, the data message is received from an operating system residing on the client.

12. The method of claim 7, wherein in scanning the data message, a scanning set of executable instructions is selectively executed to scan the data message for zero or more of the viruses.

13. The method of claim 7, wherein in receiving the data message, the data message is received as a data stream from the client and scanned as the data stream is received.

14. An email system to validate an email message, comprising:

a local email set of executable instructions residing on a client;

a remote validation set of executable instructions residing on a server; and

wherein the email message is received by the local email set of executable instructions from a sender, who intends the email message for the client and the client is who the email message is directed to for consumption, and local email set of executable instructions decrypts the email message and then streams the email message to the remote validation set of executable instructions located on the server in an unencrypted format or in a different encrypted format from what was received on the client from the sender and wherein the email message is scanned and a validation flag associated with a result of the scan is sent to the local email set of executable instructions back on the client.

15. The email system of claim 14, wherein the local email set of executable instructions accesses the email message if the result indicates the scan validated the email message.

16. The email system of claim 15, wherein the scan validates the email message if the email messages are free of viruses.

17. The email system of claim 14, wherein the local email set of executable instructions removes the data message if the flag indicates the scan did not validate the email message.

18. The email system of claim 14, wherein communications between the local email set of executable instructions and the remote validation set of executable instructions are secure.

19. The email system of claim 18, wherein public and private key pairs associated with the client and the server are used to encrypt and authenticate the communications.

20. The email system of claim 14, wherein the email message includes an attachment message and wherein the email message is in a Secure Multi-Purpose Internet Mail Extension (S/MIME) format when received by the local email set of executable instructions.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.